Algebras with finite descriptions

André Nies

The University of Auckland

August 1, 2005

Finite descriptions

- We consider algebras, that is, structures in a signature of finitely many function symbols.
- How can one describe a countably infinite algebra (usually group, ring, ...) by a finite amount of information?
- One way is giving a finite presentation (if there is one).

Two new approaches

- In the first approach, domain and functions are described by finite automata (FA). This is mostly of interest for infinitely generated algebras (at least in the case of groups).
- The second approach only applies to finitely generated algebras. The description is a single first-order sentence.

Part 1: FA-presentability

Definition

A countable structure in a finite signature is **finite-automaton presentable** (or automatic) if

- the elements of the domain can be represented by the strings in a regular language D, in a way that
- finite automata can also check if the atomic relations hold.

For checking the relations, the strings representing elements are written below each other, using symbols like $\begin{smallmatrix} a \\ b \\ a \end{smallmatrix}$ or $\begin{smallmatrix} c \\ b \\ \diamondsuit \end{smallmatrix}$ in the powers of the given alphabet. One fills up with $\diamondsuit$'s to get the same lengths.

Introduced by Hodgson (1982) for a new proof of decidability of the theory of $(\mathbb{N}, +)$; Khoussainov/Nerode (1995)

Example: $(\mathbb{N}, +)$

We represent numbers in binary, the **least** significant digit first. 0 is represented by the empty string. Thus

- The **alphabet** is $\{0, 1, \Diamond\}$
- The **domain** consists of the strings ending in 1, and the empty string
- A finite automaton checks the correctness of the sum, via the carry bit procedure, where the carry goes to the right. $\Diamond$ is treated like 0. For instance, 5+22=27 becomes:

$$\begin{array}{ccccc} 1 & 0 & 1 & \Diamond & \Diamond \\ 0 & 1 & 1 & 0 & 1 \\ \hline 1 & 1 & 0 & 1 & 1 \end{array}$$

Classes of FA-presentable structures

Each finite structure is FA-presentable.

In a sense, FA-presentability generalizes finiteness.

We will consider finitely axiomatized classes:

Boolean algebras, graphs, (abelian) groups and rings.

- Surprisingly, some turn out to be very complex: it is hard to detect if two members are isomorphic. (In a sense they have many non-isomorphic members.)
- If the class is not too complex, one can try to describe all structures in it. Example: Boolean Algebras.

Complex or simple?

For several interesting classes, for instance groups, abelian groups, and rings, we cannot decide yet if one of the extremes applies, or if the truth lies in between.

One approaches the problem from both sides:

- Find more examples of FA-presentable structures in that class
- prove limiting results for the class.

Both have been quite successful recently for abelian groups (more later). First we will classify FA-presentable Boolean Algebras.

Direct powers

Given a finite structure F, the following structure is FA-presentable:

$$F^{(\omega)} = \{g : \mathbb{N} \mapsto F \mid g \text{ is almost constant}\},$$

with the operations and relations defined componentwise.

The alphabet consists of $\Diamond$ and a symbol for each element of F.

Example: Let F be the 2-element Boolean algebra, then

$$B_{\text{fin-cof}} = F^{(\omega)}$$

is the Boolean algebra of finite or cofinite subsets of $\mathbb{N}$.

Classifying Boolean Algebras

$B_{\text{fin-cof}}$ = the Boolean algebra of finite or cofinite subsets of $\mathbb{N}$.

Theorem 1 (Khoussainov, Nies, Rubin, Stephan, 2004) *An infinite Boolean algebra B is FA-presentable iff it is isomorphic to $(B_{\textit{fin-cof}})^n$ for some n.*

$\mathrm{Th}(B)$ is decidable, being the theory of atomic Boolean Algebras.

The isomorphism problem for FA-presentations of Boolean Algebras is decidable.

Interpretations and decidability

- Given an FA-presented structure $\boldsymbol{A}$ and a formula φ (possibly with parameters), one can effectively determine an FA recognizing the relation on $\boldsymbol{A}$ defined by φ.

  (To do existential quantifiers in the inductive proof, one uses that each NFA is equivalent to a DFA.)

- So a structure interpretable in an FA-presentable structure is also FA-presentable.

- The theory of an FA-presentable structure is uniformly decidable. That is, given a presentation $\boldsymbol{A}$ and a sentence ψ, "$\boldsymbol{A} \models \psi$" is decidable.

Isom. problem for BAs

One may even allow the quantifier $\exists^\infty x$ in the formula φ. This uses that any FA-presentation contains the regular relation "x is longer than y", though it is not part of the signature.

An infinite FA-presentable Boolean algebra $\boldsymbol{A}$ is determined by the number n such that $\boldsymbol{A} \cong (B_{\text{fin-cof}})^n$, and n can be obtained effectively: Given an FA-presentation of a structure A in the signature of Boolean algebras, one can decide if A is an infinite Boolean algebra, and if so compute the largest n such that $A \models$

"there are n disjoint elements with infinitely many atoms below."

If it is finite, it isdetermined by the number of atoms. Thus the problem if two presentations describe the same structure is decidable.

A complex class

Fix a finite signature, and consider FA-presentations A, B of structures which are given by tuples of FA's. The **isomorphism problem**

$$\{\langle A, B\rangle \mid \exists f : A \cong B\}$$

is Σ^1_1.

We have seen it is decidable for BAs. In contrast, it is as hard as possible for graphs.

Theorem 2 (Khoussainov, Nies, Rubin, Stephan) *The isomorphism problem for FA-presentable graphs is Σ^1_1-complete.*

In fact, the graphs can be chosen connected and without cycles (such graphs are called successor trees).

- We code the isomorphism problem for computable subtrees R of $(\mathbb{N}^*, \preceq)$ (here $\preceq$ is the prefix ordering), which is Σ^1_1-complete. For each R we build an FA presentation of a successor tree A_R. $R \cong S \;\Leftrightarrow\; A_R \cong A_S$.

- We use that $(\mathbb{N}^*, \prec)$ has a nice FA presentation over $\{0, 1\}$: the domain D consists of the empty word λ and words that end in 1. The relation is the prefix ordering of $\{0, 1\}^*$, restricted to D.

- The recursive tree R is given by a reversible Turing machine T. T halts on $w \in D$ iff w is not in R.

- The configuration graph of T, where the edges are transitions, is FA-presentable.

- A_R is obtained form D by attaching computations of T at each element $w \in D$. Also attach finite chains of each length, and add infinitely many isolated chains of each length. Then $w \in R \;\Leftrightarrow\;$ some infinite chain starts at w. So $R \cong S \;\Leftrightarrow\; A_R \cong A_S$.

Other complex classes

- The proof can be modified to obtain undirected graphs instead of successor trees
- These can be coded into the following, preserving FA-presentability:
  - Commutative monoids
  - partial orders
  - lattices of height 4

So the isomorphism problem for FA-presentable structures in all these classes is Σ_1^1-complete.

The theory

The complexity of a class can also be measured by the computational complexity of its theory. Recall that, given an FA-presentation A and a sentence ψ, "$A \models \psi$" is decidable.

So if $\mathcal{C}$ is a finitely axiomatizable class, then

$$\mathrm{Th}(\mathcal{C} \cap \text{FA-presentable}) \text{ is } \Pi^0_1.$$

- For many interesting classes, like graphs, groups and rings, already $\mathrm{Th}(\mathcal{C} \cap \text{finite})$ is Π^0_1-complete. In fact, the valid and the finitely refutable sentences are effectively inseparable.
- In this case, also $\mathrm{Th}(\mathcal{C} \cap \text{FA-presentable})$ is Π^0_1-complete.

Abelian groups

- The theory of finite abelian groups is decidable, so the previous argument (that the theory of the FA-presentable structures in the class is complex) doesn't work here.
- It is unknown if the theory of FA-presentable abelian groups is decidable.
- We approach this class by the examples/restrictions method.

Abelian groups: Examples

We have already seen that $(\mathbb{N}, +)$ is FA-presentable. Then so is $(\mathbb{Z}, +)$, because it can be interpreted in $(\mathbb{N}, +)$. We give further examples. Let $\mathbb{Z}(m) = \mathbb{Z}/m\mathbb{Z}$ and for $k \in \mathbb{N}, k \geq 2$, let

$$R_k = \mathbb{Z}[1/k] = \{z/k^i \,:\, z \in \mathbb{Z}, i \in \mathbb{N}\}.$$

The examples are:

- $\mathbb{Z}(m)^{(\omega)}$ (direct power of finite cyclic group)
- Prüfer groups $\mathbb{Z}(k^\infty) = R_k/\mathbb{Z}$
- R_k itself

The Prüfer group $\mathbb{Z}(2^\infty)$

The **alphabet** is $\{0, 1, \Diamond\}$. Elements are represented by strings, with **most** significant digit first. For instance 101 represents [5/8]. The **domain** consists of the strings ending in 1, and the empty string to represent 0. A finite automaton checks the correctness of the sum, via the carry bit procedure, where the carry goes to the **left**. The leftmost carry is ignored. For instance, [5/8]+[1/2]=[1/8] becomes:

$$\begin{array}{ccc} 1 & 0 & 1 \\ 1 & \Diamond & \Diamond \\ \hline 0 & 0 & 1 \end{array}$$

For $\mathbb{Z}(k^\infty)$, the alphabet is $\{0, \ldots, k-1, \Diamond\}$. For R_k^+, use two tracks, one for the integers in binary, and one for the fractional part. One carry bit may move from second track to first.

Are there more examples?

- A finite product of FA-presentable structures is FA-presentable.
- Till recently, the only known FA-presentable abelian groups were the finite products of a finite abelian group and some of the examples above.
- We will obtain others: torsion-free, indecomposable and of rank 2 or higher. The (torsion-free) **rank** of an abelian group is the maximum size of a linearly independent set.

1: Finite extensions

Proposition 3 (N, Semukhin) *Let A be an abelian group with an FA-presentable subgroup of finite index. Then A is FA-presentable.*

We use this to show that an example from Fuchs [1971] is FA-presentable. Let $\boldsymbol{e}_0, \boldsymbol{e}_1$ be the standard base of $\mathbb{Q}^2$.

For $\boldsymbol{a} \in \mathbb{Q}^2$, let $p^{-\infty}a$ denote the infinite set $\{a, p^{-1}a, p^{-2}a, \ldots\}$.

Thus $\langle p^{-\infty}\boldsymbol{a}\rangle \cong R_p$ for $\boldsymbol{a} \neq 0$.

- Fix distinct primes p_0, p_1, q
- Let G be the group generated by $p_0^{-\infty}\boldsymbol{e}_0, p_1^{-\infty}\boldsymbol{e}_1$ and $q^{-1}(\boldsymbol{e}_0 + \boldsymbol{e}_1)$

G is indecomposable, that is, not a proper direct product (Fuchs).
G is FA-presentable because $\langle p_0^{-\infty}\boldsymbol{e}_0, p_1^{-\infty}\boldsymbol{e}_1\rangle$ has finite index.

2: Amalgams

Proposition 4 (N, Semukhin) *Let A, B be FA-presented subgroups of an abelian group L. Suppose that*

$$U = \{\langle x, -x \rangle : x \in A \cap B\}$$

is an FA-recognizable subset of the direct sum $A \oplus B$.

Then the subgroup $S = A + B$ of L is FA-presentable.

Proof: $S \cong$ the amalgam $A \oplus B/U$. So S can be interpreted in the FA presentable structure $(A \oplus B, +, U)$. Q.e.d.

- For a first application, let $L = \mathbb{Q}, A = R_2, B = R_3$. Then $U \cong \mathbb{Z}$ and $S \cong R_6$.
- The FA-representation obtained is different from the one of R_6 in base 6: in the latter case R_2 is not a regular subgroup.

A rank 2 rigid example

We use this to obtain a rank 2 example S which is **rigid** (the only endomorphisms are the trivial ones, multiplication by an integer). For such a group, each subgroup of finite index is indecomposable. So S cannot be obtained by the method of finite extensions.

Again work in $L = \mathbb{Q}^2$, let $\boldsymbol{e}_0, \boldsymbol{e}_1$ be the standard base of $\mathbb{Q}^2$,

and fix distinct primes p_0, p_1, q.

- Let $A = \langle p_0^{-\infty}\boldsymbol{e}_0, p_1^{-\infty}\boldsymbol{e}_1\rangle$ and $B = \langle q^{-\infty}(\boldsymbol{e}_0 + \boldsymbol{e}_1)\rangle$
- Then $A \cap B = \mathbb{Z}(\boldsymbol{e}_0 + \boldsymbol{e}_1)$

$S = \langle p_0^{-\infty}\boldsymbol{e}_0, p_1^{-\infty}\boldsymbol{e}_1, q^{-\infty}(\boldsymbol{e}_0 + \boldsymbol{e}_1)\rangle$ is rigid and FA-presentable.

The examples generalize to arbitrary finite ranks.

Abelian groups: restrictions

Theorem 5 (Khoussainov, Nies, Rubin, Stephan) *The free rank ω abelian group, that is, $(\mathbb{Q}^+, \times)$, is not FA-presentable.*

Proof uses the "explosion method": Consider an FA-presentation that contains a binary operation $\circ$, represented by NFA with k states. By the pumping Lemma,

$$|x \circ y| \leq \max\{|x|, |y|\} + k,$$

else there are infinitely many z such that $x \circ y = z$.

Using this, if $(\mathbb{Q}^+, \times)$ were FA-presentable (over alphabet Σ), then for some n, one could generate more than $|\Sigma|^{n+1}$ strings of length $\leq n$.

An open question

Question 6 *Is* $(\mathbb{Q}, +)$ *FA-presentable?*

The explosion method fails because $(\mathbb{Q}, +)$ embeds into a FA-presentable structure (A, g) with a partial binary operation g.

However, the method still shows that, in any possible presentation,

$$1/p \text{ has length} \geq p/\log p$$

for infinitely many primes p [F. Stephan, 2003]. This is much longer than we are used to from previous representations of number systems (about $\log p$).

Groups: Examples

Here are some non-abelian FA-presentable groups:

- The dyhidral group $D_{2\infty}$, an extension of $\mathbb{Z}$ by $\mathbb{Z}_2$;
- if we extend $\mathbb{Z}$ by $\mathbb{Z}$, we obtain a torsion free example:

$$\langle a, d : d^{-1}ad = a^{-1} \rangle.$$

However, both have an abelian subgroup of finite index.

Not virtually abelian

Here is a new example, from [N, R. Thomas ta]. Consider the group G presented by the following.

- Generators: x, y_i, z_i $(i \in \mathbb{N})$
- Relations:
  - $y_i^2 = z_i^2 = 1$
  - Everything commutes, except that
$$z_i^{-1} x z_i = x y_i$$
    (namely z_i conjugates x to $x y_i$).

G does not have an abelian subgroup of finite index.

Groups: restrictions

Fix a class $\mathcal{C}$ of groups closed under subgroups. G is $\mathcal{C}$-**by-finite** if G has a subgroup of finite index in $\mathcal{C}$.

Theorem 7 (Nies, Thomas, ta) *Let G be an FA-presentable infinite group. Then each finitely generated subgroup of G is abelian-by-finite.*

(In fact, the torsion-free rank of the abelian part is at most $\log(|\Sigma|)(k+1)$, where Σ is the alphabet and k the number of states to recognize the group operation.)

This improves work of Oliver/Thomas, who showed that each finitely generated FA-presentable group is abelian-by-finite.

The Heisenberg group

Recall the Heisenberg group

$$\mathrm{UT}_3(\mathbb{Z}) = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}.$$

This is the rank 2 free nilpotent group of class 2.

Elements of the proof

- By the pumping lemma, a subgroup H generated by $\{g_1, \ldots, g_r\}$ has polynomial growth, namely

$$\{t(g_1, \ldots, g_r) : |t| \leq n\} \text{ has size polynomial in } n.$$

  So by Gromov's result, it is nilpotent-by-finite

- Heisenberg alternative: a f.g. nilpotent-by-finite group either embeds $\mathrm{UT}_3(\mathbb{Z})$ or is abelian-by-finite.

- If G embeds $\mathrm{UT}_3(\mathbb{Z})$ then G is not FA-presentable. (The proof uses an explosion argument, but not for $\mathrm{UT}_3(\mathbb{Z})$ but rather a copy of $(\mathbb{N}, \times)$ defined in $\mathrm{UT}_3(\mathbb{Z})$ via commutators (Mal'cev). We have to show that this first-order definition still works in the super-group G.)

A limiting result for rings

Theorem 8 (Nies, Thomas) *If R is an FA-presentable ring with identity (possibly non-commutative), then R is locally finite.*

We show that otherwise $\mathrm{GL}_3(R)$ has a f.g. subgroup which is not abelian-by-finite. $\mathrm{GL}_3(R)$ can be interpreted in R and is therefore FA-presentable.

Question 9 *Are there FA-presentable commutative rings with 1 other than obvious variants of $F^{(\omega)}$, where F is a finite ring?*

If so, we would also obtain further examples of FA-presentable groups, for instance $\mathrm{GL}_n(R)$ and $\mathrm{UT}_n(R)$.

Part 2: q.f.a. algebras

(This part is shorter...)

Definition

Definition 10 (N, 2001) *Fix a finite signature of function symbols. An infinite f.g. algebra G is quasi-finitely axiomatizable (q.f.a.) if there is a first–order sentence φ such that*

- $G \models \varphi$
- *If H is a f.g. algebra such that $H \models \varphi$, then $G \cong H$.*

Thus the first-order axiom provides a finite description of G, given the extra information that G is f.g.

I will mainly study this property in various classes of groups: abelian, nilpotent, metabelian, and a particular type of permutation groups.

Abelian groups are not q.f.a.

- By Szmielew's quantifier elimination for the theory of abelian groups, each sentence φ which holds in an abelian group G also holds in $G \oplus \mathbb{Z}_p$, for almost all primes p.
- If G is f.g. then $G \not\cong G \oplus \mathbb{Z}_p$, so G is not q.f.a..

An algebraic characterization

Sabbagh and Oger gave an algebraic characterization of being q.f.a. for infinite nilpotent groups G. Informally, G is q.f.a. iff G is far from abelian. Let

- $G' = \langle [x, y] : x, y \in G \rangle$
- $\Delta(G) = \{x : (\exists m > 0)\ x^m \in G'\}$
  (least $N \triangleleft G$ such that G/N is torsion free abelian).

Theorem 11 (Sabbagh and Oger, 2004)

$$G \text{ is q.f.a.} \Leftrightarrow Z(G) \subseteq \Delta(G).$$

The direction $\Rightarrow$ holds for all f.g. groups.

Heisenberg group, again

Recall that $\mathrm{UT}_3(\mathbb{Z}) = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$. This group is torsion free,

and $Z(G) = G' = \begin{pmatrix} 1 & 0 & \mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

So $\mathrm{UT}_3(\mathbb{Z})$ is q.f.a. by Oger/Sabbagh. I had proved this first by a logic proof, using the interpretation of $(\mathbb{N}, +, \times)$ due to Mal'cev.

All non-abelian UT groups over $\mathbb{Z}$, and all free nilpotent non-abelian groups are q.f.a.

Metabelian q.f.a. groups

For groups G, A, C one writes $G = A \rtimes C$ if

$$AC = G,\ A \lhd G, \text{ and } A \cap C = \{1\}.$$

Give examples of q.f.a. groups that are split extensions $A \rtimes C$, A abelian, $C = \langle d \rangle$ infinite cyclic.

Theorem 12 (N) • *For each $m \geq 2$, the group*

$$H_m = \langle a, d \,|\, d^{-1}ad = a^m \rangle$$

is q.f.a. (one-relator group, first studied by Baumslag/Solitär)

- *For each prime p, the restricted wreath product $\mathbb{Z}_p \wr \mathbb{Z}$ is q.f.a. (not finitely presented)*

H_m is a split extension of $A = \mathbb{Z}[1/m] = \{zm^{-i} : z \in \mathbb{Z}, i \in \mathbb{N}\}$ by $\langle d \rangle$, where the action of d is $u \mapsto um$.

Some q.f.a. proofs

The proofs that those groups $G = A \rtimes C$ are q.f.a. follow the same scheme. The group A is given by a first-order definition. One writes a list $\psi(d) = P1 \;\&\; \ldots \& Pk$ of first-order properties of an element d in a group G so that the axiom $\exists d\, \psi(d)$ shows that the group in question is q.f.a..

Let C be the centralizer of d, namely $C = \{x : [x, d] = 1\}$. In the following, u, v denote elements of A and x, y elements of C.

(P1) The commutators form a subgroup (so G' is definable)

(P2) A and C are abelian, and $G = A \rtimes C$

(P3) $C - \{1\}$ acts on $A - \{1\}$ without fix points. That is, $[u, x] \neq 1$ for each $u \in A - \{1\}$, $x \in C - \{1\}$.

(P4) $|C : C^2| = 2$

- To specify H_m one uses the definition $A = \{g : g^{m-1} \in G'\}$, and requires in addition that

(P5) $\forall u \, d^{-1}ud = u^m$,

(P6) The map $u \mapsto u^q$ is 1-1, where q is a fixed prime not dividing m

(P7) $x^{-1}ux \neq u^{-1}$ for $u \neq 1$

(P8) $|A : A^q| = q$

(P9) d is not an i-th power for any i, $2 \leq i \leq m$.

- To specify $\mathbb{Z}_p \wr \mathbb{Z}$, one uses the definition $A = \{g : g^p = 1\}$, and requires in addition that $|A : G'| = p$ and no element in $C - \{1\}$ has order $< p$.

Complex q.f.a. groups

A set $S \subseteq \omega$ is called an **arithmetical singleton** if there exists a formula $\varphi(X)$ in the language of arithmetic extended by a new unary predicate symbol X that for each $P \subseteq \mathbb{N}$, $\varphi(P)$ is true in the standard model of arithmetic if and only if $P = S$.

Examples: all arithmetical sets; $\mathrm{Th}(\mathbb{N}, +, \times)$

Theorem 13 (Morozov, Nies, 2003) *For each arithmetical singleton $S \subseteq 3\mathbb{N}$, there exists a 3–generated q.f.a.–group G_S whose word problem $W(G)$ has the same complexity as S (namely, $S =_T W(G)$).*

G_S is the subgroup of the permutations of $\mathbb{Z}$ generated by successor, $(0, 1)$ and

$$\prod_{k \in S}(k, k+1, k+2).$$

Prime groups

A notion from model theory:

- G is **prime** if G is an elementary submodel of each H such that $\mathrm{Th}(G) = \mathrm{Th}(H)$.
- For f.g. groups, this is equivalent to: there is a generating tuple $\overline{g}$ whose orbit (under the automorphisms of G) is definable by a first order formula. (This looks a bit like the q.f.a. definition!)

Various theories fail to have one: $\mathrm{Th}(\mathbb{Z}, +, 0), \mathrm{Th}(F_2)$.

Prime vs q.f.a.

Oger and Sabbagh showed that if G is a nilpotent f.g. group, then G is q.f.a. $\Leftrightarrow$ G is prime.

Theorem 14 (N) *There are uncountably many non-isomorphic f.g. groups that are prime. (The class consists of the f.g. groups satisfying a sentence α.)*

In particular, not all prime groups are q.f.a.. The permutation groups G_S as above provide those examples (for sets S whose elements are sufficiently far apart, but not arithmetical singletons any longer).

The converse is open. However all the examples of q.f.a. groups discussed above are prime (Khelif and others).

Question 15 *Is each q.f.a. group prime?*

Q.f.a. rings

Consider commutative rings with identity. Recently Belegradek, Khelif, Sabbagh, ... have looked at the question which f.g. rings are q.f.a.

All are finitely presented. The hypothesis is they are ALL q.f.a.

So far, this has been shown for $(\mathbb{Z}, +, \times)$ and more generally for all rings whose abelian group is $\mathbb{Z}^n$ for some n.

Also for $\mathbb{Z}[X]$ and $\mathbb{Z}/d\mathbb{Z}[X]$.